



HAL
open science

Prise en compte de différents modes de défaillance des composants réseau dans l'évaluation de la fiabilité des transmissions

Damien Aza-Vallina, Bruno Denis, Jean-Marc Faure

► **To cite this version:**

Damien Aza-Vallina, Bruno Denis, Jean-Marc Faure. Prise en compte de différents modes de défaillance des composants réseau dans l'évaluation de la fiabilité des transmissions. 4èmes Journées Doctorales / Journées Nationales MACS (JD-JN-MACS'11), Jun 2011, Marseille, France. pp 263-268. hal-00588690

HAL Id: hal-00588690

<https://hal.science/hal-00588690>

Submitted on 26 Apr 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Prise en compte de différents modes de défaillance des composants réseau dans l'évaluation de la fiabilité des transmissions

Damien AZA-VALLINA¹, Bruno DENIS¹, Jean-Marc FAURE¹

¹ Laboratoire Universitaire de Recherche en Production Automatisée (LURPA)
ENS Cachan, 61 Avenue du Président Wilson, 94235 Cachan Cedex, France

{aza-vallina,denis,faure}@lurpa.ens-cachan.fr

Résumé— Ce papier présente une méthode originale pour obtenir une expression analytique de la fiabilité d'une transmission de données entre deux terminaux d'un système en réseau dans lequel les composants peuvent comporter plusieurs modes de défaillance et où certaines de ces défaillances peuvent se propager à des composants adjacents. Cette contribution est illustrée sur une architecture typique des systèmes critiques ; la comparaison à une approche classique, dans laquelle un seul mode de défaillance est retenu et la propagation des défaillances est ignorée, permet de montrer les bénéfices que procure cette proposition.

Mots-clés— Systèmes en réseau, Modèles de fautes, Propagation de faute, Sécurité, Fiabilité

I. INTRODUCTION

Dans les systèmes critiques, comme le transport ou la production d'énergie, les communications entre les éléments du système de contrôle-commande ont été historiquement réalisées à l'aide de connexions point-à-point. Les technologies basées sur le multiplexage des données, telles que CAN (Controller Area Network), FlexRay, mais aussi des solutions basées sur Ethernet telles que Ethernet/IP, Ethernet Powerlink, AFDX (Avionics Full Duplex) pour l'aéronautique, les ont partiellement remplacées, pour des raisons de réduction du coût des installations.

Parallèlement à ces développements industriels, de nombreux travaux de recherche ont été conduits afin de faciliter le développement et l'usage de ces technologies réseaux en proposant des contributions permettant l'évaluation des performances temporelles [1][2][3], de la disponibilité [4] ou de la fiabilité [5] des systèmes en réseau. Ce papier s'intéresse uniquement à cette dernière caractéristique, attribut de sûreté essentiel pour les systèmes critiques.

Les études de fiabilité d'un système en réseau s'appuient classiquement sur un modèle de composants interconnectés, parmi lesquels on distingue des équipements terminaux, émetteurs et/ou récepteurs de données tels que contrôleurs, capteurs/actionneurs intelligents, et des équipements de transmission de données, tels que concentrateurs et commutateurs. Ces composants sont alors considérés comme ayant un seul mode de défaillance [6][7], ce qui permet la modélisation du comportement de chacun d'eux sous forme d'une chaîne de Markov continue, généralement homogène, à deux états. Le calcul de la fiabilité d'une transmission entre deux terminaux du réseau, probabilité qu'il existe au

moins un chemin entre ces deux terminaux ne comportant que des composants non défaillants, repose alors sur l'analyse des chemins entre ces deux terminaux et de la chaîne de Markov représentative du comportement de ces chemins.

Cette modélisation des fautes des composants n'est cependant adaptée qu'aux composants matériels ; pour les composants qui comportent des éléments matériels et logiciels, ce qui est très fréquent pour les composants réseau concernés, des modèles de fautes plus élaborés doivent être introduits comme précisé dans [8]. Selon cette référence, un composant peut en effet être sujet à six types de fautes que l'on peut diviser en trois groupes :

- les fautes liées à la transmission d'informations : absence intempestive ou présence intempestive de transmission d'information ;
- les fautes liées à la valeur de l'information transmise (intégrité des données) : l'information transmise possède une valeur supérieure ou inférieure à la valeur réelle ;
- les fautes liées à la date de transmission : la transmission se produit trop tôt ou trop tard.

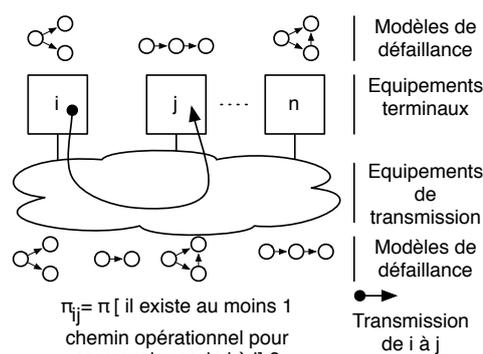


Fig. 1. Objectif de cette étude

Prendre en compte plusieurs types de fautes implique que la chaîne de Markov représentant chacun des composants sera plus complexe et que le calcul de la fiabilité d'une transmission devra être modifié pour tenir compte de l'impact des nouveaux modes de défaillance sur la transmission de données. L'objet de cette communication (Fig. 1) est de proposer une nouvelle méthode de calcul de fiabilité, adaptée à des composants à plus d'un mode de défaillance.

Les modèles des composants et de la topologie du réseau sont présentés dans la section suivante, tandis que la méthode de calcul de la fiabilité d'une transmission intégrant ces modèles est détaillée en section III. L'application de cette contribution à une étude de cas permet, dans la section IV, d'en montrer l'intérêt.

II. MODÉLISATION DES ÉLÉMENTS DU PROBLÈME

Cette section présente dans un premier temps le modèle de la topologie d'un réseau de communication retenu. Une modélisation générique du comportement d'un composant réseau est ensuite proposée.

A. Modélisation de la topologie du réseau

Un réseau de communication peut être modélisé sous la forme d'un graphe non orienté noté $G = (\mathcal{N}, E)$ où :

- \mathcal{N} est un ensemble des nœuds, un nœud représentant un composant du réseau.
- E est un ensemble d'arcs non orientés entre des couples d'éléments de \mathcal{N} . Un arc représente une liaison physique entre deux composants réseau distincts.

Dans ce graphe, l'ensemble des chemins qui permettent d'assurer la transmission entre deux nœuds i et j sera noté P_{ij} ; il pourra être composé d'un ou plusieurs chemins qui seront notés P_{ij}^k .

Deux nœuds sont dit adjacents si il existe un arc qui les relie.

B. Modélisation du comportement d'un composant

Usuellement, les composants sont souvent considérés comme ayant un seul mode de défaillance; ils sont alors fonctionnels ou non. Si cette modélisation peut sembler appropriée au premier abord, elle n'est pas adaptée à des composants plus élaborés qui sont composés d'une partie matérielle et logicielle. C'est pour cela qu'il est nécessaire d'introduire un modèle de défaillance plus complet.

La modélisation d'un composant se fera donc par une chaîne de Markov continue MC_i (Cassandras et Lafortune [9]) :

$$MC_i = \langle X_i, p_i, \pi_i^0 \rangle \quad (1)$$

Où :

- X_i est l'ensemble des états de la chaîne de Markov,
- p_i est la matrice de transition,
- $\pi_i(0)$ est le vecteur de probabilité d'occupation des états à l'instant initial.

Cette chaîne peut comporter plus de deux états, selon le nombre de défaillances retenues pour la modélisation. Cependant, ses états peuvent être regroupés en trois sous-ensembles qui forment une partition sur X_i :

- X_i^0 sous-ensemble des états de bon fonctionnement,
- X_i^P sous-ensemble des états de défaillances propageantes. Une défaillance d'un composant i sera qualifiée de propageante lorsque son occurrence entraîne l'impossibilité d'assurer toute transmission pour tout composant k adjacent à i , même si ce composant k n'est pas défaillant.
- X_i^F sous-ensemble des états de défaillances non propageantes. Une défaillance non propageante, quand elle

se produit, n'a aucun effet sur les composants adjacents.

avec $X_i^0 \cap X_i^F = X_i^0 \cap X_i^P = X_i^F \cap X_i^P = \emptyset$ et $X_i^0 \cup X_i^F \cup X_i^P = X_i$

La probabilité que l'état actif à l'instant t soit l'état α sera notée $\pi_i^\alpha(t)$; la probabilité que l'état actif à l'instant t appartienne à l'un des trois sous-ensembles X_i^0, X_i^F, X_i^P sera notée respectivement $\pi_i^{X_i^0}(t), \pi_i^{X_i^F}(t), \pi_i^{X_i^P}(t)$.

Pour la suite de ce papier, certaines restrictions ont été apportées à ce modèle :

- Le nombre d'états de bon fonctionnement est limité à un ($card(X_i^0) = 1$).
- Les composants sont considérés comme non réparables; il n'existe pas de transition partant d'un état de défaillance vers l'état de bon fonctionnement.
- Les états de défaillance sont persistants; il n'existe pas de transition entre deux états de défaillance.

Avec l'ensemble de ces hypothèses, le comportement d'un composant est décrit par le modèle de la figure 2(a), si tous les états de bon fonctionnement et de défaillance sont explicités, ou de la figure 2(b) si on se limite à une description par les trois sous-ensembles d'états précédemment définis. On notera enfin que cette modélisation ne comporte pas d'états de fonctionnement dégradé : le composant est soit opérationnel (ou en bon fonctionnement), soit défaillant, la défaillance pouvant n'affecter que le composant considéré, soit ce composant et ses voisins immédiats lorsqu'elle est de nature propageante.

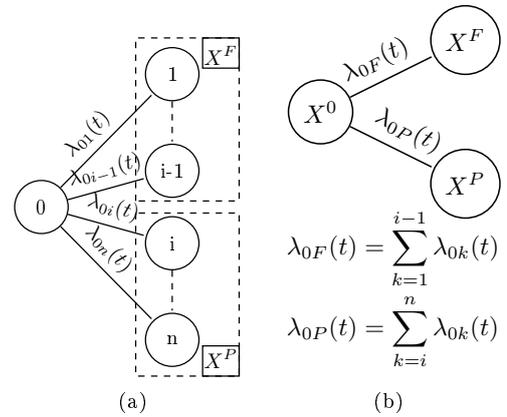


Fig. 2. Modélisation du comportement d'un composant (λ_{XY} : taux de défaillance)

III. EVALUATION DE LA FIABILITÉ D'UNE TRANSMISSION

A partir des modélisations présentées dans la section précédente, une méthode de calcul de la fiabilité d'une transmission entre deux nœuds terminaux i et j , probabilité à l'instant t qu'il existe au moins un chemin permettant d'assurer la transmission de données entre ces deux nœuds, a été élaborée. Cette méthode a pour objectif de fournir une expression analytique de la fiabilité. Elle vise également à éviter la composition des chaînes de Markov représentant le comportement des composants réseau afin de s'affranchir du classique problème d'explosion combinatoire qui se produit lors de la composition de modèles à états.

Cette méthode comporte trois étapes qui sont effectuées séquentiellement :

A Recherche, pour chacun des chemins de longueur minimale entre i et j , des combinaisons d'états des composants telles que la transmission par ce chemin soit possible.

B Détermination, pour l'ensemble des chemins de longueur minimale entre i et j , des combinaisons d'états des composants telles que la transmission possible.

C Détermination de l'expression analytique de la fiabilité de la transmission.

Ces trois étapes vont être détaillées dans les sous-sections suivantes et seront illustrées par un exemple issu de [10] (Fig. 3(a)). Il s'agit d'une architecture réseau composée de trois terminaux CAN interconnectés par deux étoiles (média redondé), chaque étoile étant assurée par un concentrateur.

Le modèle de la topologie de ce réseau est donné figure 3(b). Le graphe comporte 5 nœuds ($\mathcal{N} = \{a, b, c, d, e\}$), a, b, c pour les terminaux et d, e pour les concentrateurs.

Dans la suite on s'intéresse à la transmission de données entre les terminaux a et b , c'est à dire entre les nœuds a et b du graphe.

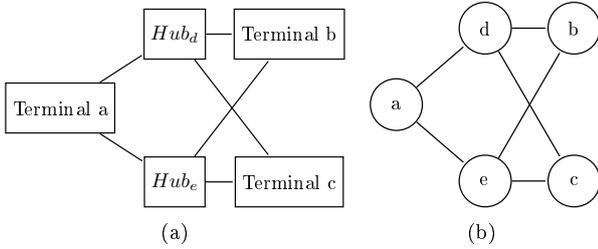


Fig. 3. Architecture physique (a) avec 5 composants dont la topologie est modélisée par le graphe (b)

A. Recherche des combinaisons d'états des composants pour un chemin¹

Pour qu'une transmission par le chemin P_{ij}^k entre les nœuds i et j soit possible il faut à la fois que :

- tous les composants représentés par un nœud appartenant au chemin P_{ij}^k soient dans leur état de bon fonctionnement,
- tous les composants représentés par un nœud adjacent à un nœud du chemin P_{ij}^k soient dans leur état de bon fonctionnement ou dans un état de défaillance non propageante,
- tous les autres composants soient dans un état quelconque.

En notant N_{ij}^k l'ensemble des nœuds qui appartiennent au chemin P_{ij}^k et PN_{ij}^k l'ensemble des nœuds adjacents à un nœud du chemin P_{ij}^k , l'ensemble des états admissibles, états tels que la transmission soit possible par le chemin P_{ij}^k , pour un composant représenté par un nœud l ($l \in \mathcal{N}$), est noté $X_l^{P_{ij}^k}$, avec :

$$X_l^{P_{ij}^k} = \begin{cases} X_l^0 & \text{si } l \in N_{ij}^k \\ X_l^0 \cup X_l^F & \text{si } l \in PN_{ij}^k \\ X_l & \text{sinon} \end{cases} \quad (2)$$

1. Par souci de concision, le terme "chemin" désignera un chemin de longueur minimale dans ce qui suit

Pour le cas support, il y a deux chemins notés P_{ab}^1 et P_{ab}^2 qui permettent d'assurer la transmission entre les nœuds a et b (Fig. 4). Les états admissibles des composants pour que la transmission soit possible par chacun des chemins sont définis par (2) et sont présentés dans la table I.

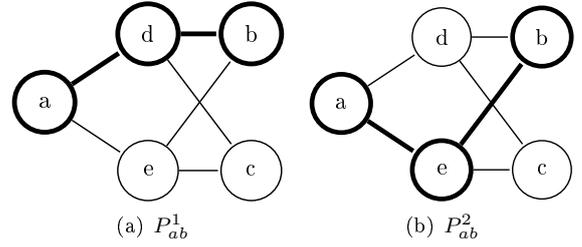


Fig. 4. Les deux chemins permettant d'assurer la transmission entre a et b

Composant	Chemin	
	P_{ab}^1	P_{ab}^2
a	X_a^0	X_a^0
b	X_b^0	X_b^0
c	$X_c^0 \cup X_c^F$	$X_c^0 \cup X_c^F$
d	X_d^0	$X_d^0 \cup X_d^F$
e	$X_e^0 \cup X_e^F$	X_e^0

TABLE I
ENSEMBLE DES ÉTATS ADMISSIBLES DES COMPOSANTS
EN FONCTION DU CHEMIN

Les composants a et b doivent être dans leur état de fonctionnement (X_a^0 et X_b^0) quelque soit le chemin. A contrario, le composant c qui n'est jamais sur un chemin de transmission mais qui est systématiquement adjacent à un composant du chemin (adjacent à d pour le chemin P_{ab}^1 et à e pour P_{ab}^2) ne doit pas être dans un état de défaillance qui se propage, $X_c^{P_{ab}^1} \notin X_c^P$ c'est à dire $X_c^{P_{ab}^1} \in X_c - X_c^P = X_c^0 \cup X_c^F$.

L'état du réseau à un instant donné est la combinaison des états actifs des composants à cet instant ; une combinaison caractéristique de l'état du réseau comporte donc n termes, avec $n = \text{card}(\mathcal{N})$. L'ensemble des combinaisons admissibles pour une transmission selon un chemin s'obtient alors à partir des ensembles d'états admissibles des composants de la façon suivante :

$$C_{ij}^{P_{ij}^k} = \prod_{l \in \mathcal{N}} X_l^{P_{ij}^k} \quad (3)$$

Pour la transmission entre a et b , ces ensembles sont, pour les deux chemins :

$$C_{ab}^{P_{ab}^1} = X_a^0 \times X_b^0 \times (X_c^0 \cup X_c^F) \times X_d^0 \times (X_e^0 \cup X_e^F) \quad (4)$$

$$C_{ab}^{P_{ab}^2} = X_a^0 \times X_b^0 \times (X_c^0 \cup X_c^F) \times (X_d^0 \cup X_d^F) \times X_e^0 \quad (5)$$

On pourra noter que chacun de ces ensembles comporte 4 éléments.

B. Détermination des combinaisons d'états des composants pour la transmission

L'ensemble des états admissibles d'un composant peut dépendre du chemin étudié; un composant peut par exemple appartenir à un chemin P_{ij}^m et être adjacent à un composant du chemin P_{ij}^n , P_{ij}^m et P_{ij}^n étant deux chemins pouvant assurer la transmission étudiée. L'ensemble des combinaisons d'états admissibles pour tous les chemins, noté C_{ij} , s'obtient donc en faisant l'union des ensembles des combinaisons admissibles pour chaque chemin. D'où :

$$C_{ij} = \bigcup_{P_{ij}^k} C_{ij}^{P_{ij}^k} \quad (6)$$

Pour l'exemple, cet ensemble est obtenu à partir de (4) et (5). Il vient alors :

$$C_{ab} = X_a^0 \times X_b^0 \times (X_c^0 \cup X_c^F) \times [(X_d^0 \times X_e^0) \cup (X_d^F \times X_e^0) \cup (X_d^0 \times X_e^F)] \quad (7)$$

On pourra remarquer que cet ensemble comporte 6 combinaisons d'états parmi les 243 (3^5) que contient la chaîne de Markov décrivant le comportement du réseau. Les étapes A et B ont donc permis d'éviter la construction de ce modèle à états de taille non triviale même pour un exemple simple.

C. Expression analytique de la fiabilité de la transmission

Soit c une combinaison d'états des composants et α_l^c l'état du composant l dans cette combinaison. La probabilité du réseau d'être dans cette combinaison à l'instant t est notée $\pi^c(t)$. Sachant que la probabilité que le composant l soit dans un état α_l^c est notée $\pi_l^{\alpha_l^c}(t)$ alors $\pi^c(t)$ se calcule de la manière suivante :

$$\pi^c(t) = \prod_{l \in \mathcal{N}} \pi_l^{\alpha_l^c}(t) \quad (8)$$

La fiabilité de la transmission ($\pi_{ij}(t)$) est alors la somme des probabilités de chacune des combinaisons d'états admissibles :

$$\pi_{ij}(t) = \sum_{c \in C_{ij}} \pi^c(t) = \sum_{c \in C_{ij}} \prod_{l \in \mathcal{N}} \pi_l^{\alpha_l^c}(t) \quad (9)$$

Pour le cas support, la fiabilité de la transmission entre les nœuds a et b est donc :

$$\pi_{ab} = \pi_a^{X_a^0} \cdot \pi_b^{X_b^0} \cdot (\pi_c^{X_c^0} + \pi_c^{X_c^F}) \cdot [(\pi_d^{X_d^0} \cdot \pi_e^{X_e^0}) + (\pi_d^{X_d^F} \cdot \pi_e^{X_e^0}) + (\pi_d^{X_d^0} \cdot \pi_e^{X_e^F})] \quad (10)$$

Une application de cette méthode à une architecture réseau comportant un bus redondé est proposée dans la section suivante. Cette étude de cas permet en particulier de montrer l'intérêt de la modélisation comportementale proposée par rapport à une approche classique où chaque composant ne comporte qu'un seul mode de défaillance.

IV. APPLICATION

L'utilisation d'une architecture de type bus pour supporter les communications dans un système critique n'est envisageable que si le medium est redondé. La méthode décrite dans la section précédente sera donc illustrée ici sur l'exemple générique de la figure 5 qui comporte n terminaux reliés par deux bus B1 et B2, supposés identiques. On ne considèrera dans cette étude qu'un seul mode de défaillance pour chacun des bus et deux modes de défaillance pour chacun des terminaux. Après avoir présenté les modèles comportementaux des composants de ce réseau, les trois étapes de la méthode seront détaillées. La comparaison des résultats obtenus à ceux résultant d'une modélisation à un seul mode de défaillance pour chaque composant permettra de montrer l'intérêt de la modélisation proposée en II.

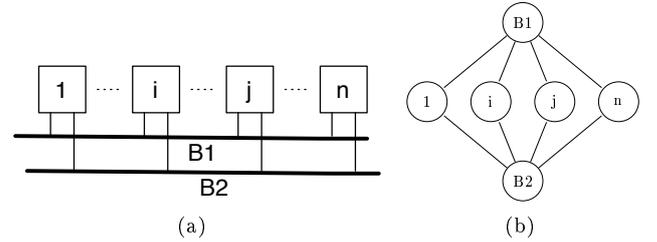


Fig. 5. Bus redondé (a) et modèle de sa topologie (b)

A. Modélisation du comportement des composants

Avec les hypothèses faites sur le nombre de modes de défaillance pour les deux classes de composants, deux types de modèles comportementaux doivent être utilisés.

A.1 Composant à un seul mode de défaillance

Dans ce cas, le comportement du composant est décrit par une chaîne de Markov à deux états (Fig. 6(a)) : un état représentatif du bon fonctionnement, noté x^{OK} , et un état représentatif de la défaillance, supposée non propageante, noté x^F . Il vient alors : $X_l = \{x_l^{OK}, x_l^F\}$, $X_l^0 = \{x_l^{OK}\}$, $X_l^F = \{x_l^F\}$ et $X_l^P = \emptyset$.

On admettra également que cette chaîne de Markov est homogène; le taux de défaillance λ_l est donc constant et les probabilités d'occupation des deux états à l'instant t sont :

$$\begin{cases} \pi_l^{X_l^0}(t) = e^{-\lambda_l \cdot t} \\ \pi_l^{X_l^F}(t) = 1 - e^{-\lambda_l \cdot t} \end{cases} \quad (11)$$

A.2 Composant à plusieurs modes de défaillance

Les deux modes de défaillance suivants sont retenus :

- absence intempestive de transmission, caractérisé par le fait qu'un composant ne communique pas alors qu'il le devrait. Ce mode ne se propage pas aux composants adjacents et sera représenté par un état x_l^F .
- présence intempestive de transmission, qui se caractérise à l'inverse par le fait qu'un composant communique alors qu'il ne le devrait pas; les défaillances étant considérées comme persistantes, cette communication intempestive est maintenue continuellement, monopolisant le médium de transmission. Ce mode de défaillance se propage aux composants adjacents et sera

représenté par un état x_l^P .

Le comportement du composant est donc décrit par une chaîne de Markov à trois états (Fig. 6(b)) tels que :

$$X_l = \{x_l^{OK}, x_l^F, x_l^P\}, X_l^0 = \{x_l^{OK}\}, X_l^F = \{x_l^F\} \text{ et } X_l^P = \{x_l^P\}$$

En admettant que cette chaîne est homogène, les taux de défaillance λ_l^f et λ_l^p sont constants et les probabilités d'occupation des trois états à l'instant t sont :

$$\begin{cases} \pi_l^{X_l^0}(t) = e^{-(\lambda_l^o + \lambda_l^p) \cdot t} \\ \pi_l^{X_l^F}(t) = \frac{\lambda_l^f}{\lambda_l^p + \lambda_l^f} \cdot (1 - e^{-(\lambda_l^f + \lambda_l^p) \cdot t}) \\ \pi_l^{X_l^P}(t) = \frac{\lambda_l^p}{\lambda_l^p + \lambda_l^f} \cdot (1 - e^{-(\lambda_l^f + \lambda_l^p) \cdot t}) \end{cases} \quad (12)$$

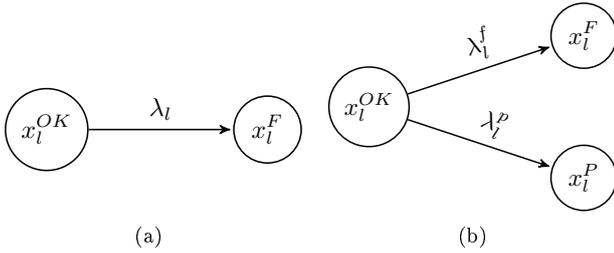


Fig. 6. Modèle comportemental de composant à un mode (a) et à deux modes de défaillance (b)

B. Evaluation de la fiabilité d'une transmission

Cette analyse sera conduite sur l'exemple de la transmission entre les terminaux 1 et n ; la transposition à tout autre couple de terminaux est immédiate.

B.1 Recherche des combinaisons d'états des composants pour un chemin

Deux chemins, notés P_{1n}^1 et P_{1n}^2 , permettent d'assurer la transmission entre les nœuds 1 et n (Fig. 7).

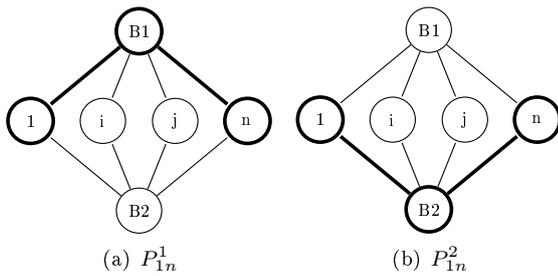


Fig. 7. Les deux chemins permettant d'assurer la transmission entre 1 et n

Pour chacun de ces chemins et pour chaque composant, il est alors possible de déterminer les ensembles d'états admissibles à partir de (2); la table II contient le résultat de cette analyse.

Les nœuds 1 et n appartiennent au chemin, quel qu'il soit; ils doivent donc être dans leur état de bon fonctionnement. A l'opposé, les nœuds 2 à $n-1$ n'appartiennent pas au chemin utilisé mais sont systématiquement adjacents au bus, quel que soit ce chemin; ils ne doivent donc pas être dans un état de défaillance qui se propage, la communication intempestive correspondante empêchant alors

Composant	Chemin	
	P_{1n}^1	P_{1n}^2
1	X_1^0	X_1^0
$l \in \{2 \dots n-1\}$	$X_l^0 \cup X_l^F$	$X_l^0 \cup X_l^F$
n	X_n^0	X_n^0
B1	X_{B1}^0	$X_{B1}^0 \cup X_{B1}^F$
B2	$X_{B2}^0 \cup X_{B2}^F$	X_{B2}^0

TABLE II

ENSEMBLE DES ÉTATS ADMISSIBLES D'UN COMPOSANT EN FONCTION DU CHEMIN

les nœuds 1 et n d'accéder au bus. L'expression des ensembles C_{1n}^1 et C_{1n}^2 est alors :

$$C_{1n}^{P_{1n}^1} = X_1^0 \times \left[\prod_{l=2}^{n-1} (X_l^0 \cup X_l^F) \right] \times X_n^0 \times X_{B1}^0 \times (X_{B2}^0 \cup X_{B2}^F) \quad (13)$$

$$C_{1n}^{P_{1n}^2} = X_1^0 \times \left[\prod_{l=2}^{n-1} (X_l^0 \cup X_l^F) \right] \times X_n^0 \times (X_{B1}^0 \cup X_{B1}^F) \times X_{B2}^0 \quad (14)$$

Pour chacun de ces ensembles, il n'y a qu'un seul état admissible, l'état de bon fonctionnement, pour trois composants (1, n et un bus en fonction du chemin considéré) et deux états admissibles pour $n-1$ composants ($n-2$ terminaux et le bus non utilisé). Leur cardinalité est donc : $card(C_{1n}^{P_{1n}^1}) = card(C_{1n}^{P_{1n}^2}) = 1^3 \cdot 2^{n-1} = 2^{n-1}$.

B.2 Détermination des combinaisons d'états des composants pour la transmission

L'ensemble C_{1n} des combinaisons d'états admissibles pour la transmission est l'union des deux ensembles $C_{1n}^{P_{1n}^1}$ et $C_{1n}^{P_{1n}^2}$, c.a.d.

$$C_{1n} = X_1^0 \times \left[\prod_{l=2}^{n-1} (X_l^0 \cup X_l^F) \right] \times X_n^0 \times [(X_{B1}^0 \times (X_{B2}^0 \cup (X_{B1}^0 \times X_{B2}^F) \cup (X_{B1}^F \times X_{B2}^0)))] \quad (15)$$

Cet ensemble contient $3 \cdot 2^{n-2}$ combinaisons à comparer aux $2^2 \cdot 3^n$ combinaisons possibles avec les modèles comportementaux de composants utilisés. Pour un réseau à 10 terminaux par exemple, on obtient 768 combinaisons admissibles, alors que la construction de la chaîne de Markov décrivant le comportement complet du réseau conduirait à un modèle à 236 196 états, soit plus de 300 fois plus.

B.3 Expression analytique de la fiabilité de la transmission

Connaissant l'ensemble des combinaisons d'états de composants admissibles, la fiabilité de la transmission étudiée s'exprime en fonction des probabilités d'occupation des états de la façon suivante :

$$\begin{aligned} \pi_{1n}(t) = & \pi_1^{X_1^0}(t) \cdot \left[\prod_{l=2}^{n-1} (\pi_l^{X_l^0}(t) + \pi_l^{X_l^F}(t)) \right] \cdot \pi_n^{X_n^0}(t) \\ & \cdot \left[(\pi_{B1}^{X_{B1}^0}(t) \cdot \pi_{B2}^{X_{B2}^0}(t)) + (\pi_{B1}^{X_{B1}^0}(t) \cdot \pi_{B2}^{X_{B2}^F}(t)) \right. \\ & \left. + (\pi_{B2}^{X_{B2}^F}(t) \cdot \pi_{B2}^{X_{B2}^0}(t)) \right] \end{aligned} \quad (16)$$

Etant donné les modèles proposés en A et en particulier les expressions (11) et (12), l'expression analytique de la fiabilité recherchée est :

$$\begin{aligned} \pi_{1n}(t) = & e^{-(\lambda_1^f + \lambda_1^p) \cdot t} \cdot \left[\prod_{l=2}^{n-1} \left(\frac{\lambda_l^f + \lambda_l^p \cdot e^{-(\lambda_l^f + \lambda_l^p) \cdot t}}{\lambda_l^f + \lambda_l^p} \right) \right] \\ & \cdot e^{-(\lambda_1^f + \lambda_n^p) \cdot t} \cdot \left[(e^{-\lambda_{B1} \cdot t} \cdot e^{-\lambda_{B2} \cdot t}) \right. \\ & \left. + (e^{-\lambda_{B1} \cdot t} \cdot (1 - e^{-\lambda_{B2} \cdot t})) + ((1 - e^{-\lambda_{B1} \cdot t}) \cdot e^{-\lambda_{B2} \cdot t}) \right] \end{aligned} \quad (17)$$

Il convient de souligner nettement que cette expression dépend du nombre de terminaux connectés au bus. La fiabilité d'une transmission n'est donc pas indépendante de ce nombre, avec le modèle comportemental de terminal introduit.

B.4 Application numérique

En supposant que tous les terminaux ont les mêmes taux de défaillance et en prenant les valeurs suivantes pour les taux de défaillance :

$$\begin{aligned} - \lambda_{B1, B2} &= 10^{-7} h^{-1} \\ - \lambda_l^f &= 8.10^{-8} h^{-1} \text{ et } \lambda_l^p = 2.10^{-8} h^{-1} \end{aligned}$$

l'application numérique de l'expression (17), pour trois valeurs de n : 2, 5 et 10, permet de représenter l'évolution de la fiabilité en fonction du temps (Fig. 8).

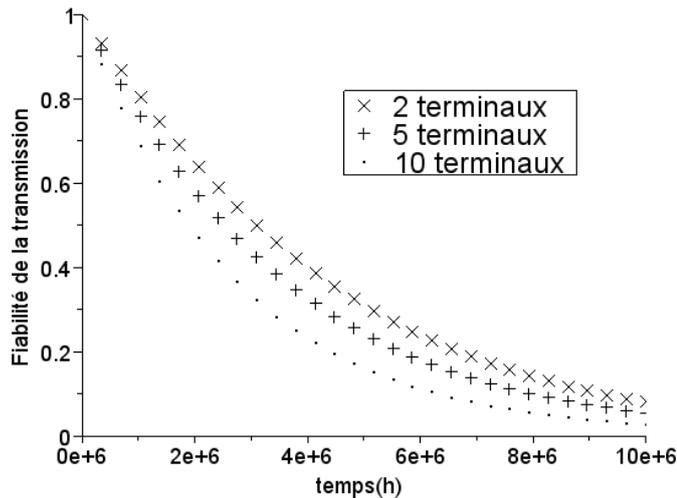


Fig. 8. Fiabilité de la transmission entre deux terminaux en fonction du temps et du nombre de terminaux connectés au bus (2,5,10).

La figure 8 montre clairement que la fiabilité dépend du nombre de terminaux, comme l'indique l'équation (17). Augmenter le nombre de terminaux connectés aux bus conduit à une diminution de la fiabilité, car de nouvelles défaillances pouvant se propager sont introduites.

Une méthode d'évaluation de la fiabilité d'une transmission entre deux terminaux d'un réseau de communication a été proposée dans ce papier. L'originalité de cette proposition est qu'elle considère que certains composants du réseau peuvent défaillir de plusieurs manières, en devenant par exemple silencieux ou bavards, et que certaines de ces défaillances peuvent se propager aux composants adjacents, les rendant inutilisables pour la transmission de données même s'ils n'ont pas de défaillance propre.

Cette méthode fournit une expression analytique de la fiabilité, ce qui permet par exemple d'analyser l'évolution au cours du temps de cet attribut de sûreté dans une perspective de maintenance. Cette expression analytique est établie à partir de la connaissance des combinaisons d'états admissibles, qui permettent la transmission; elles sont déduites de l'analyse de la topologie du réseau et non par composition de chaînes de Markov, afin d'éviter (ou limiter) l'explosion combinatoire.

Les perspectives de ces travaux concernent tout d'abord la création de modèles comportementaux de composants plus riches que ceux actuellement développés, en distinguant par exemple les états où le composant est actif, utilisé pour la transmission de données, ou dormant, en attente d'une sollicitation. Il sera alors possible de s'intéresser à l'application de ces propositions lors de la conception de réseaux pour systèmes critiques.

RÉFÉRENCES

- [1] Gaëlle MARSAL : *Evaluation of Time Performances of Ethernet-based Automation Systems by Simulation of High-level Petri Nets*. Shaker Verlag GmbH, Germany, Aachen, Germany, Germany, 2007.
- [2] Jean-Philippe GEORGES, Nicolas KROMMENACKER, Thierry DIVOUX et Eric RONDEAU : A design process of switched Ethernet architectures according to real-time application constraints. *Engineering Applications of Artificial Intelligence*, 19(3):335-344, 04 2006.
- [3] Henri BAUER, Jean-Luc SCHARBARG et Christian FRABOUL : Improving the worst-case delay analysis of an AFDX network using an optimized trajectory approach. *IEEE Transactions on Industrial Informatics*, 6(4):521-533, 10 2010.
- [4] Steve LIMAL : *Architectures de contrôle-commande redondantes à base d'Ethernet Industriel : modélisation et validation par model-checking temporel*. Thèse de doctorat, École Normale Supérieure de Cachan - ENS Cachan, 01 2009.
- [5] Mohammad GHASEMZADEH, Christoph MEINEL et Sara KHANJI : K-terminal network reliability evaluation using Binary Decision Diagram. *In 3rd International Conference on Information and Communication Technologies : From Theory to Applications (ICTTA)*, pages 1-5, 2008.
- [6] Michael O. BALL : Computing network reliability. *Operations Research*, 27(4):823-838, 07-08 1976.
- [7] Arnie ROSENTHAL : Computing the reliability of complex networks. *SIAM Journal on Applied Mathematics*, 32(2):pp. 384-393, 1977.
- [8] Yannis PAPADOPOULOS, Audrey TRAN, Jean-Marc FAURE et Christian GRANTE : Component Failure Behaviour : Patterns and Reuse in Automated System Safety Analysis. *In Proceedings of SAE 2006*, pages paper n° 06AE-287, Detroit États-Unis, 04 2006.
- [9] Christos G. CASSANDRAS et Stephane LAFORTUNE : *Introduction to Discrete Event Systems*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.
- [10] M. BARRANCO, L. ALMEIDA et J. PROENZA : Recancentrate : a replicated star topology for can networks. *In Emerging Technologies and Factory Automation, 2005. ETFA 2005. 10th IEEE Conference on*, volume 2, pages 8 pp. 468-476, sept. 2005.